



COURS DE GESTION DES DROITS D'ACCÈS

SÉRIE N° 01

OBJECTIF PÉDAGOGIQUE :

À la fin de cette série, le stagiaire doit être capable d'expliquer les différentes permissions des droits d'accès pour les comptes, et les groupes utilisateurs.

PLAN DE LA LEÇON :

I- PLANIFICATION

- 1- Convention de nomenclature (dénomination)
- 2- Règles concernant les mots de passe
- 3- Emplacement des dossiers de base

QUESTIONS DE COURS

SOLUTIONS

II- LE GESTIONNAIRE D'UTILISATEURS POUR LES DOMAINES

III- CRÉATION ET CONFIGURATION D'UN COMPTE

- 1-** Station de travail
- 2-** Le compte utilisateur
- 3-** Profils
- 4-** L'identification SID (Système d'identification)

IV- COMPTES UTILISATEURS PRÉDÉFINIS

V- OPÉRATIONS SUR UN COMPTE UTILISATEUR

- 1-** Renommer un compte utilisateur
- 2-** Copier des comptes utilisateur du domaine

CONCLUSION

I- PLANIFICATION :

Un compte d'utilisateur permet à un utilisateur d'ouvrir une session sur des domaines et des ordinateurs sous une identité qu'il est possible d'authentifier et d'autoriser pour un accès aux ressources du domaine.

Pour rendre plus efficace le processus de création de comptes d'utilisateur, vous devez connaître les conventions et les consignes déjà utilisées sur le réseau. Vous pouvez gérer plus facilement les comptes d'utilisateur si ces conventions et consignes ont été respectées lors de la création de ces comptes.

1- Convention de nomenclature (dénomination) :

La convention de dénomination établit le mode d'identification des comptes d'utilisateur dans un domaine. Une convention de dénomination cohérente permet de mémoriser plus aisément les noms d'ouverture de session des utilisateurs, et de les repérer dans des listes.

Sur un réseau qui prend en charge un grand nombre d'utilisateurs, il est recommandé de suivre la convention de dénomination déjà utilisée.

Respectez les instructions ci-dessous concernant les conventions de dénomination :

- Les noms d'ouverture de session des comptes d'utilisateur de domaine doivent être uniques dans Active Directory.
- Les noms complets des comptes d'utilisateur de domaine doivent être uniques dans le domaine dans lequel vous créez le compte d'utilisateur.
- Les noms des comptes d'utilisateur locaux doivent être uniques sur l'ordinateur sur lequel vous créez le compte d'utilisateur local.
- Les noms d'ouverture de session de l'utilisateur peuvent contenir jusqu'à 20 caractères majuscules et minuscules (le champ accepte plus de 20 caractères, à l'exception des caractères suivants : \ / [] : ; | = , + * ? < > Vous pouvez utiliser une combinaison de caractères spéciaux et alphanumériques pour permettre d'identifier de façon unique les comptes d'utilisateur.

2- Règles concernant les mots de passe :

Pour protéger l'accès au domaine ou à un ordinateur, tous les comptes d'utilisateur doivent disposer d'un mot de passe complexe. Cela permet d'empêcher des personnes non autorisées d'ouvrir des sessions sur votre domaine.

Pour affecter des mots de passe aux comptes d'utilisateur, prenez en compte les instructions ci-dessous :

- Affectez toujours un mot de passe complexe au compte Administrateur pour éviter tout accès non autorisé à ce compte.
- Déterminez si les mots de passe seront construits par vous-même ou par les utilisateurs.
- Vous pouvez affecter des mots de passe uniques aux comptes d'utilisateur, et empêcher les utilisateurs de les modifier, ou vous pouvez permettre à ceux-ci d'entrer le mot de passe de leur choix lors de leur première ouverture de session.
- Dans la plupart des cas, il est conseillé de laisser aux utilisateurs le contrôle de leur mot de passe.
- Expliquez aux utilisateurs l'importance d'employer un mot de passe complexe, difficile à deviner.
- Evitez d'utiliser des mots de passe représentant une association évidente, par exemple le prénom d'un membre de la famille de l'utilisateur.
- Utilisez de longs mots de passe, ils seront d'autant plus difficiles à trouver. Les mots de passe peuvent comporter jusqu'à 128 caractères. Il est recommandé d'utiliser au minimum 8 caractères.
- Utilisez une combinaison de lettres majuscules et minuscules, ainsi que des caractères non alphanumériques.

Exemple de mot de passe difficile à deviner : **gsopnb123/ATUI/549**

3- Emplacement des dossiers de base :

Vous pouvez fournir aux utilisateurs un emplacement central sur le réseau qui leur permettra de stocker leurs documents. Cet emplacement supplémentaire constitue le dossier de base de chaque utilisateur.

Les dossiers de base ne font pas partie d'un profil d'utilisateur, et n'ont donc pas d'incidence sur le processus d'ouverture de session. Vous pouvez placer les dossiers de base de tous les utilisateurs à un emplacement central sur un serveur réseau.

Prenez en compte les points ci-dessous lors du choix de l'emplacement du dossier de base :

- **Capacité de sauvegarde et de restauration**, votre principale responsabilité consiste à éviter toute perte de données, Il est beaucoup plus facile de s'assurer que les fichiers sont sauvegardés lorsqu'ils se trouvent à un emplacement central sur un serveur.
- **Espace disponible suffisant sur le serveur**, Il est important que le serveur dispose de suffisamment de place pour que les utilisateurs puissent y stocker leurs données. Grâce aux quotas de disque, qui permettent de surveiller et de limiter la quantité d'espace disque disponible pour chaque utilisateur.
- **Espace disponible suffisant sur l'ordinateur de l'utilisateur**, si les utilisateurs travaillent sur des ordinateurs disposant de très peu d'espace disque ou sans disques durs, les dossiers de base doivent être situés sur un serveur réseau.
- **Performances du réseau**, le trafic réseau est moins élevé si les dossiers de base sont situés sur l'ordinateur local de l'utilisateur.

Pour créer un dossier de base, suivez la procédure ci-dessous :

- a) Créez un dossier sur un serveur, puis partagez-le.
- b) Accordez l'autorisation appropriée pour ce dossier.
- c) Fournissez au compte d'utilisateur le chemin d'accès du dossier.

QUESTIONS DE COURS :

- 1- Suggérez une convention de dénomination afin de gérer les utilisateurs qui porte le même prénom.
- 2- Suggérez une convention afin de gérer les comptes utilisateurs temporaire dans une entreprise.
- 3- Quels sont les points à prendre en considération lors du choix de l'emplacement du dossier de base ?

SOLUTIONS :

- 1- Si les utilisateurs sont très nombreux, votre convention de dénomination pour l'ouverture de session doit prendre en compte les employés homonymes. Voici une suggestion pour gérer les homonymies :

Utilisez le prénom et l'initiale du nom, puis ajoutez des lettres supplémentaires du nom pour différencier les homonymes. Par exemple, pour deux utilisatrices appelées **Julie Loup**, le nom d'ouverture de session du compte d'utilisateur de la première peut être **Juliel**, et celui de la seconde **Julielo**.

- 2- Dans certaines entreprises, il est utile d'identifier les employés temporaires par leur compte d'utilisateur. Pour ce faire, vous pouvez faire précéder le nom du compte d'utilisateur par un T et un trait d'union. Par exemple, T-Juliel.
- 3- Points à prendre en compte lors du choix de l'emplacement du dossier de base :
 - Capacité de sauvegarde et de restauration.
 - Espace disponible suffisant sur le serveur.
 - Espace disponible suffisant sur l'ordinateur de l'utilisateur.
 - Performances du réseau.

II-LE GESTIONNAIRE D'UTILISATEURS POUR LES DOMAINES :

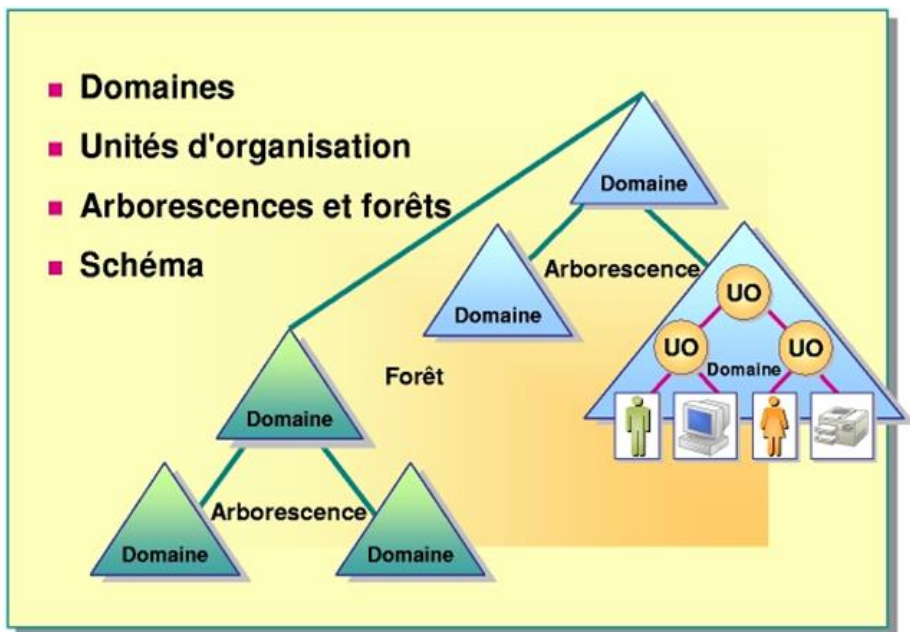
Pour gérer les utilisateurs de domaine, créez des comptes d'utilisateurs dans les services de domaine Active Directory (AD DS).

AD DS fournit une base de données distribuée qui stocke et gère des informations sur les ressources réseau et les données spécifiques à des applications provenant d'applications utilisant un annuaire. Les administrateurs peuvent utiliser AD DS pour organiser les éléments d'un réseau, tels que les utilisateurs, les ordinateurs et les autres périphériques, en une structure hiérarchique de type contenant-contenu. La structure hiérarchique de type contenant-contenu inclut la forêt Active Directory, les domaines inclus dans la forêt et les unités d'organisation (OU) de chaque domaine. Un serveur qui exécute AD DS est nommé contrôleur de domaine.

L'organisation des éléments d'un réseau en une structure hiérarchique de type contenant-contenu offre les avantages suivants :

- La forêt agit comme une limite de sécurité pour une organisation et définit l'étendue de l'autorité des administrateurs. Par défaut, une forêt contient un domaine unique, appelé également domaine racine de la forêt.
- Des domaines supplémentaires peuvent être créés dans la forêt pour assurer le partitionnement des données AD DS, ce qui permet aux organisations de répliquer des données uniquement là où cela est nécessaire. Cela permet le dimensionnement global des services de domaine Active Directory (AD DS) sur un réseau disposant d'une bande passante limitée. Un domaine Active Directory prend en charge également plusieurs autres fonctions principales liées à l'administration, dont notamment l'identité des utilisateurs, l'authentification et les relations d'approbation à l'échelle du réseau.
- Les unités d'organisations (UO) simplifient la délégation de l'autorité pour faciliter la gestion d'un grand nombre d'objets. Par le biais de la délégation, des propriétaires peuvent transférer une autorité complète ou limitée sur des objets à

d'autres utilisateurs ou groupes. La délégation est importante car elle aide à distribuer la gestion d'un grand nombre d'objets à plusieurs personnes chargées d'effectuer des tâches de gestion.



III- CRÉATION ET CONFIGURATION D'UN COMPTE :

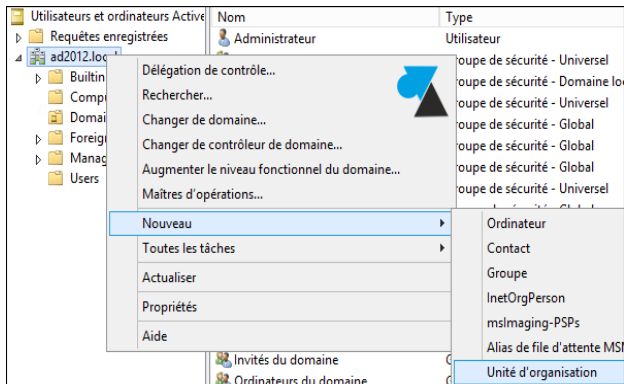
1- Station de travail :

Les comptes d'ordinateur sont créés au moyen de l'outil AD DS **Ajouter des stations de travail au domaine**. Donc ajouter une station de travail sur le domaine, revient à créer un compte d'ordinateur.

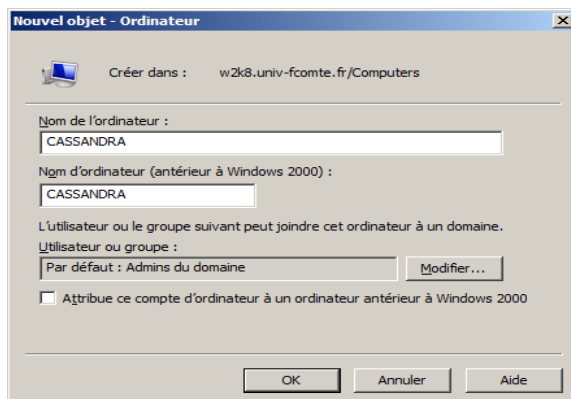
Tous les serveurs exécutant Windows Server 2003, Windows Server 2008 ou Windows Server 2008 R2 qui joignent un domaine possèdent un compte d'ordinateur. Comme les comptes d'utilisateurs, les comptes d'ordinateurs permettent d'authentifier et d'auditer l'accès au réseau et aux ressources de domaine. Chaque compte d'ordinateur doit être unique.

Pour créer des comptes d'ordinateur standard avec la console Utilisateurs et ordinateurs Active Directory, procédez de la manière suivante :

- Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez droit sur le conteneur dans lequel vous souhaitez placer le compte d'ordinateur.



- Cliquez sur **Nouveau**, puis sur **Ordinateur** :
- La boîte de dialogue Nouvel objet – Ordinateur, apparaît. Saisissez le nom de l'ordinateur client.
- Par défaut, seuls les membres du groupe Admins du domaine peuvent joindre des ordinateurs au domaine. Pour autoriser un utilisateur ou un groupe différent à effectuer cette opération, cliquez sur Modifier.



- Utilisez ensuite la boîte de dialogue **Sélectionnez Utilisateur ou Groupe** pour sélectionner un compte d'utilisateur ou de groupe.

Remarque : Vous pouvez sélectionner un compte d'utilisateur ou de groupe existant : ainsi, vous pourrez déléguer l'autorité pour joindre ce compte d'ordinateur au domaine.

- Si les systèmes Windows NT peuvent se servir de ce compte, cochez la case *Attribue ce compte d'ordinateur à un ordinateur antérieur à Windows 2000*.
- Cliquez deux fois sur **Suivant** puis sur **Terminer**.

2- Le compte utilisateur :

Vous devez créer un compte utilisateur pour chaque utilisateur qui souhaite utiliser les ressources du réseau. Les comptes utilisateur de domaine se créent à l'aide de la console **Utilisateurs et ordinateurs Active Directory**, et les comptes utilisateur locaux à l'aide de **Utilisateurs et groupes locaux**.

❖ Créer un compte utilisateur de domaine :

Il existe deux moyens de créer un nouveau compte de domaine :

- Créer un compte utilisateur **entièrement nouveau**. Pour créer un compte utilisateur entièrement nouveau, cliquez droit sur le conteneur où le placer, pointez sur Nouveau, puis sur Utilisateur. La fenêtre de l'Assistant Nouvel objet – Utilisateur s'ouvre. Lors de la création d'un nouveau compte, le système utilise les paramètres par défaut.



- Créer un nouveau compte utilisateur à partir d'un compte existant Dans **Utilisateurs et ordinateurs Active Directory**, cliquez droit sur le compte utilisateur à copier, puis sélectionnez Copier. L'Assistant Copier l'objet – Utilisateur démarre ; il est similaire à la boîte de dialogue Nouvel utilisateur. Toutefois, lors de la copie d'un compte, la plupart des paramètres du nouveau compte proviennent du compte existant (on verra ça plus en détails dans la suite de ce cour).

Lorsque l'assistant Nouvel objet (Utilisateur ou Copier l'objet) Utilisateur est lancé, créez le compte :

- Comme le montre la figure, la première boîte de dialogue de l'assistant vous permet de configurer le nom complet et le nom d'ouverture de session de l'utilisateur.

Créer dans : tunitpro.com/Users

Prénom : Ahmed Initiales :

Nom : Malek

Nom complet : Ahmed Malek

Nom d'ouverture de session de l'utilisateur :
 ahmed.malek@tunitpro.com

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
 TUNITPRO\ahmed.malek

< Précédent Suivant > Annuler

- Saisissez les nom et prénom dans les champs fournis. Ces derniers servent à créer le Nom complet, c'est-à-dire le nom d'affichage.
- Modifiez le champ Nom complet si nécessaire. Par exemple, entrez le nom au format Nom Prénom ou au format Prénom Nom. Le Nom complet doit être unique dans le domaine et ne pas comporter plus de 64 caractères.
- Saisissez le Nom d'ouverture de session de l'utilisateur dans le champ éponyme. Dans la liste déroulante, sélectionnez le domaine auquel associer le compte. Ainsi, le nom d'ouverture de session complet est défini.
- Les 20 premiers caractères du nom d'ouverture de session servent à définir le nom d'ouverture de session pré-Windows 2000. Ce nom doit être unique dans le domaine. Si nécessaire, modifiez-le.
- Cliquez sur Suivant. Configurez alors le mot de passe de l'utilisateur à l'aide des options suivantes :
 - **Mot de passe** Mot de passe du compte. Il doit respecter les conventions de votre stratégie de mots de passe.
 - **Confirmer le mot de passe** Pour garantir que le mot de passe a été correctement attribué. Saisissez-le simplement une seconde fois.
 - **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session** Si cette case est cochée, l'utilisateur doit changer le mot de passe lorsqu'il ouvrira une session.
 - **L'utilisateur ne peut pas changer de mot de passe** Si cette case est cochée, elle interdit à l'utilisateur de modifier son mot de passe.
 - **Le mot de passe n'expire jamais** Si cette case est cochée, le mot de passe de ce compte n'expire jamais. Ce paramètre remplace la stratégie de compte du domaine. Il n'est généralement pas conseillé d'activer cette option car elle réduit la sécurité apportée par les mots de passe.
 - **Le compte est désactivé** Si cette case est cochée, le compte est désactivé et ne peut être utilisé. Employez-la pour interdire temporairement l'accès à un compte.

- Cliquez sur **Suivant**, puis sur **Terminer** pour créer le compte. Si vous rencontrez des problèmes lors de sa création, un message vous en avertit et vous devez entrer à nouveau les informations des boîtes de dialogue **nom** et **mot de passe** de l'utilisateur avec le bouton **Précédent**.

Une fois le compte est créé, vous pourrez configurer les paramètres avancés qu'on verra dans la suite de cette cour.

❖ **Créer un compte utilisateur local :**

Les comptes utilisateur locaux se créent à l'aide de l'utilitaire **Utilisateurs et groupes locaux**. Pour y accéder et créer un compte :

- Cliquez sur **Démarrer, Programmes, Outils d'administration**, puis **Gestion de l'ordinateur**. Vous pouvez également sélectionner **Gestion de l'ordinateur** dans le dossier **Outils d'administration**.
- Cliquez droit sur l'entrée **Gestion de l'ordinateur** de l'arborescence de la console, puis sélectionnez **Se connecter à un autre ordinateur** dans le menu contextuel. Vous pouvez alors choisir le système dont vous souhaitez gérer les comptes locaux. Les contrôleurs de domaine n'ont pas d'utilisateurs et de groupes locaux.
- Développez le nœud **Outils système** en cliquant sur le signe plus (+) qui le joute, puis sélectionnez **Utilisateurs et groupes locaux**.
- Cliquez droit sur **Utilisateurs**, puis sélectionnez **Nouvel utilisateur**. Voici les différents champs de la boîte de dialogue **Nouvel utilisateur** :
 - **Nom d'utilisateur** Nom d'ouverture de session du compte utilisateur. Il doit respecter les conventions de la stratégie de nom d'utilisateur local.
 - **Nom complet** Nom complet de l'utilisateur, par exemple William R. Stanek. **Description** Description de l'utilisateur. Elle contient habituellement une description de son poste, Webmaster par exemple. Vous y ajoutez le service auquel il est attaché.

- **Mot de passe** Mot de passe du compte. Il doit respecter les conventions de votre stratégie de mots de passe.
- **Confirmer le mot de passe** Pour garantir que le mot de passe a été correctement attribué. Saisissez-le simplement une seconde fois.
- **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session** Si cette case est cochée, l'utilisateur doit changer le mot de passe lorsqu'il ouvrira une session.
- **L'utilisateur ne peut pas changer de mot de passe** Si cette case est cochée, elle interdit à l'utilisateur de modifier son mot de passe.
- **Le mot de passe n'expire jamais** Si cette case est cochée, le mot de passe de ce compte n'expire jamais. Ce paramètre remplace la stratégie de compte du domaine. **Le compte est désactivé** Si cette case est cochée, le compte est désactivé et ne peut être utilisé. Employez-la temporairement pour interdire l'accès à un compte par exemple.

➤ Cliquez sur **Créer**.

3- Profils :

Un profil d'utilisateur est créé à la première ouverture de session de l'utilisateur sur un ordinateur.

Tous les paramètres propres à l'utilisateur sont automatiquement enregistrés dans le sous-dossier de cet utilisateur dans le dossier Documents and Settings (C:\Documents and Settings\utilisateur).

Lorsque l'utilisateur ferme la session, son profil d'utilisateur est mis à jour sur l'ordinateur sur lequel il avait ouvert la session.

Le profil d'utilisateur conserve donc les paramètres de bureau de l'environnement de travail de chaque utilisateur sur l'ordinateur local.

Les types de profils d'utilisateur sont présentés ci-dessous. :

- **Profil d'utilisateur par défaut.** Ce profil est la base de tous les profils d'utilisateur. à l'origine, chaque profil d'utilisateur est une copie du profil d'utilisateur par défaut, qui est stocké sur tous les ordinateurs exécutant Windows 2000 Professionnel ou Windows 2000 Server (ou une version plus récente).
- **Profil d'utilisateur local.** Ce profil est créé la première fois qu'un utilisateur ouvre une session sur un ordinateur, et est stocké sur l'ordinateur local. Toutes les modifications apportées au profil d'utilisateur local sont propres à l'ordinateur sur lequel les changements ont été effectués. Plusieurs profils d'utilisateur locaux peuvent exister sur un ordinateur.
- **Profil d'utilisateur itinérant.** Ce profil est créé par l'administrateur système et stocké sur un serveur. Ce profil est disponible chaque fois qu'un utilisateur ouvre une session sur un ordinateur sur le réseau. Si un utilisateur apporte des modifications aux paramètres de bureau, son profil d'utilisateur est mis à jour sur le serveur lorsqu'il ferme la session.
- **Profil d'utilisateur obligatoire.** Ce profil est créé par l'administrateur pour indiquer les paramètres particuliers d'un utilisateur ou d'utilisateurs, et peut être de type local ou itinérant. Un profil d'utilisateur obligatoire ne permet pas à un utilisateur d'enregistrer des modifications apportées aux paramètres de son bureau. L'utilisateur peut modifier les paramètres du bureau de l'ordinateur sur lequel il a ouvert une session, mais ces modifications ne sont pas enregistrées lorsqu'il la ferme. Seuls les administrateurs système sont autorisés à modifier les profils d'utilisateur obligatoires.

4- L'identification SID (Système d'identification) :

Bien que Windows Server 2008 affiche les noms d'utilisateurs pour décrire les privilèges et les autorisations, les principaux identificateurs des comptes sont les SID (security ID, identificateur de sécurité), des identificateurs uniques générés lors de la création

des comptes. Ils se composent du préfixe SID du domaine et d'un RID (relative ID, ID relatif) unique, alloué par le maître des ID relatifs.

Windows Server 2008 se sert de ces identificateurs pour gérer les comptes indépendamment des noms d'utilisateurs. Les SID ont plusieurs objectifs, notamment de vous permettre de changer facilement les noms d'utilisateurs et de pouvoir supprimer des comptes sans vous soucier du fait qu'une personne puisse obtenir l'accès aux ressources en créant simplement un nouveau compte avec le même nom.

Lorsque vous modifiez un nom d'utilisateur, vous demandez à Windows Server 2008 de mapper un SID particulier en un nouveau nom. Lorsque vous supprimez un compte, vous indiquez à Windows Server 2008 qu'un SID particulier n'est plus valide. Ensuite, même si vous créez un compte avec le même nom utilisateur, le nouveau compte ne disposera pas des mêmes privilèges et autorisations que le précédent, car le nouveau compte possède un nouveau SID.

IV- COMPTES UTILISATEURS PRÉDÉFINIS :

Plusieurs comptes utilisateurs prédéfinis sont installés avec Windows Server 2008, dont Administrateur et Invité. Avec les serveurs membres, les comptes prédéfinis sont locaux par rapport au système individuel sur lequel ils sont installés. Les comptes prédéfinis ont des équivalents dans Active Directory.

Ces comptes ont accès à l'ensemble du domaine et sont entièrement séparés des comptes locaux dans les systèmes individuels.

✓ Le compte Administrateur

Le compte prédéfini Administrateur dispose d'un accès complet aux fichiers, répertoires, services et autres ressources. Vous ne pouvez ni le supprimer, ni le désactiver. Dans Active Directory, ce compte dispose de l'accès et des privilèges complets sur l'ensemble du domaine. Sinon, il n'a généralement accès qu'au système local. Bien que les fichiers et répertoires puissent être temporairement isolés du compte Administrateur, ce dernier peut en reprendre le contrôle à tout moment en modifiant leurs autorisations d'accès.

✓ Sécurité

Afin de protéger le système ou le domaine des accès non autorisés, assurez-vous de donner au compte Administrateur un mot de passe particulièrement sécurisé. Comme il s'agit d'un compte connu de Windows, vous préférerez peut-être le renommer à titre de précaution supplémentaire. Ce faisant, créez un compte Administrateur neutre, c'est-à-dire sans permissions, droits, ni privilèges et désactivez-le.

Il n'est pas fréquent d'avoir à modifier les paramètres de base du compte Administrateur. Vous pouvez cependant modifier ses paramètres avancés, comme l'appartenance à des groupes particuliers. Par défaut, le compte Administrateur d'un domaine fait partie des groupes suivants : Administrateurs, Admins du domaine, Utilisateurs du domaine, Administrateurs de l'entreprise, Propriétaires créateurs de la stratégie de groupe et Administrateurs du schéma. La section suivante présente ces groupes de manière plus détaillée.

❖ Le compte Invité

Le compte Invité est conçu pour les utilisateurs qui ont besoin d'un accès exceptionnel ou ponctuel. Bien que les invités ne disposent que de privilèges système limités, vous devez vous montrer prudent quant à l'utilisation de ce compte. Chaque fois que vous l'utilisez, vous exposez le système à des risques de sécurité. C'est pourquoi le compte est désactivé lors de l'installation de Windows Server 2008.

Le compte Invité est, par défaut, membre des groupes Invités du domaine et Invités. Il est important de noter que le compte Invité, comme tous les autres comptes nommés, est aussi membre du groupe implicite Tout le monde qui a normalement accès par défaut à des fichiers et à des dossiers. Le groupe Tout le monde possède également des droits par défaut.

✓ Sécurité

Si vous décidez d'activer le compte Invité, assurez-vous de restreindre son usage et de modifier régulièrement son mot de passe. Comme dans le cas du compte Administrateur, vous préférerez peut-être le renommer à titre de précaution supplémentaire.

V-OPÉRATIONS SUR UN COMPTE UTILISATEUR :

1- Renommer un compte utilisateur :

La console **Utilisateurs et ordinateurs Active Directory** vous aide à renommer les comptes utilisateurs avec une boîte de dialogue **Modification du nom de l'utilisateur** pour renommer un compte utilisateur et tous les composants du nom associés. Voici comment renommer un compte :

- Recherchez le compte utilisateur à renommer dans la console Utilisateurs et ordinateurs Active Directory.
- Cliquez droit sur le compte utilisateur et choisissez **Renommer**. Le nom du compte est mis en surbrillance et prêt à être modifié. Appuyez sur la touche RETOUR ARRIÈRE ou SUPPR pour effacer le nom existant, puis appuyez sur ENTRÉE pour ouvrir la boîte de dialogue **Modification du nom de l'utilisateur**.
- Apportez les modifications nécessaires aux informations associées au nom de l'utilisateur et cliquez sur **OK**. Si l'utilisateur est connecté, un message d'avertissement vous indique que l'utilisateur doit fermer puis rouvrir sa session à l'aide du nouveau nom d'ouverture de session.
- Le compte est renommé, sans toutefois modifier le SID des autorisations d'accès. Il se peut qu'il soit nécessaire de modifier d'autres données liées à l'utilisateur dans la boîte de dialogue **Propriétés** :
 - **Chemin du profil** Modifiez le chemin du profil dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le dossier du disque correspondant.
 - **Script d'ouverture de session** Si vous employez des scripts d'ouverture de session individuels pour chaque utilisateur, modifiez le nom du script d'ouverture de session dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le script d'ouverture de session du disque.

- **Dossier de base** Modifiez le chemin d'accès du dossier de base dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le dossier du disque correspondant.

Remarque :

Modifier les informations relatives au fichier et au dossier d'un compte lorsque l'utilisateur est connecté peut occasionner des problèmes. Il est donc préférable de mettre ces informations à jour en dehors des heures de bureau ou de demander à l'utilisateur de se déconnecter quelques minutes. Dans la plupart des cas, il est possible d'écrire un petit script Windows qui effectuera les tâches pour vous rapidement et automatiquement.

2- Copier des comptes utilisateur du domaine :

Créer entièrement des comptes utilisateurs du domaine peut s'avérer fastidieux. Partez d'un compte existant plutôt que d'en recréer à chaque fois :

Cliquez droit sur le compte à copier dans Utilisateurs et ordinateurs Active Directory, puis sélectionnez Copier. La boîte de dialogue Copier l'objet – Utilisateur apparaît.

Créez le compte comme vous le feriez pour tout autre compte utilisateur du domaine. Procédez ensuite à une mise à jour des propriétés du compte, selon vos besoins. Comme vous pouvez l'imaginer, lorsque vous créez la copie d'un compte, la console Utilisateurs et ordinateurs Active Directory ne conserve pas toutes les informations provenant du compte existant. Elle essaie au contraire de ne copier que les informations nécessaires et efface celles que vous devrez mettre à jour. Les propriétés suivantes sont conservées :

- Informations relatives à la ville, au code postal et au pays définies dans l'onglet Adresse.
- Service et société dans l'onglet Organisation.

- Options du compte définies à l'aide des champs Options de compte dans l'onglet Compte.
- Horaires d'accès et stations de travail accessibles autorisées.
- Date d'expiration du compte.
- Appartenances du compte à des groupes.
- Paramètres du profil.
- Privilèges d'appels entrants.

Remarque :

Si des variables d'environnement spécifient les paramètres du profil du compte original, ces variables sont également intégrées à la copie du compte. Par exemple, si le compte original emploie la variable % User Name%, la copie du compte l'emploie également.

CONCLUSION :

À travers la série suivante, nous avons pu voir les notions de base liée aux comptes utilisateur sur Windows server, ces connaissances vont être mises en pratique à travers les TPs qui vont suivre.